‘Live life in all its' fullness’

WOODSIDE C.E.(VC) PRIMARY SCHOOL

E-Safety Policy

School expectations and guidance for staff and governors on the use of communication technologies

2021-2022

Date Ratified:	March 2022
Date Due for Review:	March 2023
Signed Head Teacher:	
Signed Chair of LAB **(where appropriate):**	

Love **R**espect **H**ope **F**orgiveness **C**hallenging Injustice

1. The Policy

Our E-Safety Policy is part of a group of ICT security and Child Protection Policies, as well as other relevant documents. Please read this policy in conjunction with the following policies: Staff (and volunteer) Acceptable Use Policy Agreement, Pupil and Parent Acceptable Use Policy, Sexting Policy, Health, Safety and Wellbeing Policy, GDPR Privacy Notice, Safeguarding Policy and KCSIE policy.

It has been compiled by the Headteacher using guidance from the government, Warwickshire LA, and the NSPCC.

- It will be reviewed annually.

The Purpose and Scope of this Policy

Internet use is a necessary tool for education, business and social interaction and is an entitlement for pupils. Our school has a duty to equip children with the skills, knowledge and understanding to be able to use the Internet safely at school, home and in the wider world.

We aim:

- To educate pupils about e-safety issues and appropriate behaviours so that they remain safe and legal online.
- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.
- To keep any personal data and information secure.
- To minimise the risks of handling sensitive information.

Through this – and other policies - we will endeavour to provide a safe and secure learning environment for children and adults. However, we cannot guarantee complete safety from inappropriate material. The responsibility must lie with everyone.

Roles and Responsibilities

<u>LAB- Governors:</u>

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

<u>Headteacher and Senior Leaders:</u>

- The Headteacher is responsible for ensuring the e-safety of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role using Smooth wall. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
- The Headteacher and Senior Leaders should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Notify parents of current developments and issues in e-safety.

The E-Safety Co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school E-Safety Policy and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with BDMAT IT team.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Monitors teaching and learning of e-safety across the school.

2. Teaching and Learning using the Internet

Teaching and Support Staff

- Have an up to date awareness of e-safety matters and report any suspected misuse or problem to the E-Safety Co-ordinator and/or Headteacher.
- Have read, understood and signed the school Staff Acceptable Use Policy.
- Monitor ICT activity in lessons, extra-curricular and extended school activities
- The school Internet is accessed using safe search engines (https://primaryschoolict.com/ and www.kidrex.org and includes appropriate content filtering.
- Children will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- If children are directed to websites as part of home learning, they will have been checked for appropriateness by the teacher setting the learning.
- When children join Woodside, parents and carers will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- If staff or pupils discover unsuitable sites or images, it will be reported to the E-Safety Co-ordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will receive regular e-safety guidance through a sequence of age-appropriate lessons.

3. Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.

- E-mails sent to external organisations should be written carefully and authorised before sending.
- Chain letters, spam, advertising, and all other emails from unknown sources will be deleted without opening or forwarding.

4. Social Networking

- Use of social networking sites such as Facebook, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider appropriate action to be taken to protect pupils and staff against cyber bullying and defamatory comments.

5. Mobile Phones

As many mobile phones have access to the internet and picture/ video messaging, which present opportunities for unrestricted access to the Internet and sharing of images, there are risks of mobile bullying, or inappropriate contact.

- Pupils by permission can bring mobile phones onto the school site where it is seen by the school and parents as a safety precaution. These are handed into the school office at the start of the school day and collected at the end of the day.
- Staff should always use the school phone or school mobile phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom during teaching hours. All staff should ensure that their phones are turned off and stored safely away during the teaching day. Staff may use their mobile phones **in the staff room or school office, during the lunch and break period**
- Parents can use mobile phones to take pictures / videos of the children if permission has been given by a member of staff. E.g. during class performances. Where permission is given for the use of mobile phones, the Headteacher or member of staff will inform parent(s)/carers(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

6. Digital/Video Cameras/ I Pads

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use the camera or video on iPads unless specifically authorised by staff.

- Publishing of images, video and sound will follow the policy set out in this document under 'Published Content'.
- Parents will use cameras, mobile phones or video equipment at school only if specifically authorised to do so by a member of staff.
- Parents can use digital /video cameras to take pictures / videos of the children if permission has been given by a member of staff. E.g. during class performances. Where permission is given for the use of digital/video cameras, the Headteacher or member of staff will inform parent(s)/carers(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

7. Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff and pupils' personal information will not be published.

8. Published Content and the School Website

- The Headteacher & School Admin Assistant will take overall editorial responsibility and ensure that content on the school website is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website or Twitter, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site and Twitter.
- Work can only be published with the permission of the pupil and parents.
- Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.
- The Governing Body may ban the use, in school, of photographic equipment by any parent who does not follow the school policy.

9. Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly by BDMAT IT team.
- Security strategies will be discussed with the trust- BDMAT.
- Updates to our E-safety system will be discussed with BDMAT IT team and implemented as appropriate.

10. Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998, GDPR and Freedom of Information Act.

11. Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and continually changing nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will use the E-Safety Incident Log Book to audit ICT use and establish if the e-safety policy is adequate. Changes to the policy and to e-safety procedures will be made as required.

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.

12. Handling E- Safety Incidents

- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents involved with the incident will be informed of the complaints procedure.
- E-safety incidents should be recorded on C Poms during the E Safety category and assigned to the Headteacher.

13. Communication of Acceptable Use Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff:

- All staff will be asked to read and sign the Staff (and Volunteer) Acceptable Use Policy Agreement.

Parents:

- Parents will be informed of the school Acceptable Use Policy when children join the school and will be informed of any updates and changes.

Approved by Chair of LAB…………………………………… date…………………

Headteacher……………………………………………………… date…………………

Review Date: March 2023